

Mise en Œuvre d'une Authentification Centrale et Unique à l'Université

Jean-Christophe Gay

DSI - Université Paris Dauphine - PSL
place du Maréchal de Lattre de Tassigny
75116 Paris

Vincent Bruhier

DSI - Université Paris Dauphine - PSL

Martial Lebec

DSI - Université Paris Dauphine - PSL

Résumé

L'annuaire électronique central de l'université (LDAP/Supann) a été mis en place en 2009 à l'université Paris Dauphine. Il est le référentiel des identités numériques pour les authentifications et le référentiel des structures de l'établissement. Depuis 2010 l'équipe Annuaire réalise un travail de fond pour que cet annuaire soit exhaustif et « temps réel ». Sur cet annuaire ont déjà été adossés diverses authentifications (SASL/mail, CAS/web, SAML/Shibboleth, Radius/Eduroam...).

Nous cherchons à mettre en place une solution d'authentification centrale et unique pour tous les services numériques de l'université. Dans cette optique nous avons décidé d'utiliser les protocoles CAS et Kerberos, CAS pour les applications web, et Kerberos pour les systèmes d'exploitation.

Nous avons déployé une infrastructure d'authentification composée de plusieurs briques : OpenLDAP, KDC, serveur CAS, domaines AD. Pour faciliter l'authentification Kerberos dans les différentes composantes de l'université nous avons créé un domaine Active Directory central fédérant les identités pour les machines Windows. L'interopérabilité entre le royaume Kerberos central et les royaumes Windows et Posix, est réalisé grâce à des relations de confiance inter-royaume.

L'utilisation du protocole Kerberos permet de renforcer la sécurité autour des mots de passe. La centralisation de l'authentification nous a permis de mettre en place un système de gestion des mots de passes et des logins uniques. Cette interface est l'unique point d'accès de l'utilisateur à son mot de passe, et nous permet d'imposer une politique de sécurité sur le mot de passe plus restrictive que précédemment. Les fonctionnalités de SSO sont utilisées pour permettre l'accès à des ressources informatiques (espace disque réseau, accès au poste de travail...).

Mots clefs

Authentification centrale, Authentification unique, Kerberos, CAS, SSO.

Introduction

La DSI de l'université Paris Dauphine s'est engagée dans une réorganisation de la gestion des identités numériques. Nous entendons par « identité numérique » l'ensemble des informations contenues dans notre SI concernant une personne physique ou morale. L'identité numérique d'un individu regroupe, entre autres, les informations d'authentification et l'appartenance à des groupes. La gestion des identités numériques regroupe l'ensemble des actions possibles sur une identité numérique, de sa création à sa destruction en incluant les opérations de mises à jours régulières. Le terme « annuaire » (ou annuaire électronique central) fait référence à un annuaire LDAP [1], permettant de stocker des fiches relatives aux identités numériques. L'authentification est l'action de vérification de l'identité d'un utilisateur.

Il y a quatre ans le référentiel des identités numériques de l'université était éparse et incomplet, malgré les efforts mis en place par la DSI autour de l'annuaire électronique central. Depuis 2009 l'équipe annuaire réalise un travail de fond

d'épuration et d'exhaustivité des informations qu'il contient. En 2012 nous faisons le constat suivant : l'annuaire électronique central était un référentiel utilisé pour la messagerie électronique et quelques applications pédagogiques. Mais dans de nombreux départements de l'université cet annuaire était sous employé, chacun préférant alimenter son système d'authentification et de gestion des identités.

De ces comportements découlaient des nombreuses problématiques d'authentification, chaque étudiant pouvant avoir jusqu'à 4 ou 5 identifiants pour accéder aux différents systèmes d'information subsistants dans les différentes composantes. L'étudiant avait alors 4 ou 5 guichets différents pour régler le problème d'authentification, sans réellement savoir vers lequel se tourner.

En 2011 nous avons été très impressionnés par les présentations autour de Kerberos faites au JRES [2] et publiée dans la presse [3]. Les mises en œuvres présentées nous ont fait réfléchir sur la pertinence de la mise en place d'une authentification Kerberos à l'université. La mise en place d'un système de mot de passe unique permettrait de résoudre le problème de prolifération des mots de passe ainsi que le problème de guichet de réponse aux utilisateurs.

Début 2012 nous lançons le projet « Passeport Dauphine », projet ayant pour but la mise en place d'une authentification unique et globale pour l'Université. Dans un premier temps nous vous présenterons ce projet, ses objectifs et ses étapes. Ensuite nous présenterons la solution que nous avons déployée à l'Université Paris Dauphine. Nous détaillerons par la suite les différentes opérations menées pour que la nouvelle infrastructure soit utilisée par les usagers pour finir par quelques perspectives pour l'avenir.

1 Unification des authentifications

Le projet « Passeport Dauphine » a pour but d'unifier l'ensemble des authentifications et de fédérer l'ensemble des identités numériques à l'université. Depuis 2009 le but de l'équipe annuaire est de rassembler l'ensemble des identités numériques dans l'annuaire électronique central. Cet objectif n'est pas encore atteint aujourd'hui, malgré la somme d'efforts mis en place. Certaines composantes de l'université continuent à faire de la résistance et à maintenir des référentiels distincts. En 2012 nous dénombrions cinq domaines Active Directory sans liens entre eux, permettant à des utilisateurs de s'authentifier sur des machines. Existait alors un domaine pour les services communs, un domaine pour le département d'éducation permanente, un domaine pour chacun des deux CRIO¹ fournissant des postes Windows et un dernier pour le service de documentation. Un effort a été fait pour unifier les logins des utilisateurs, mais aucun n'avait été fait pour unifier les mots de passes (surtout pour des raisons de confidentialité des mots de passes).

Nous voyions alors l'unification du mot de passe des utilisateurs comme un levier pour achever la fédération des identités numériques dans notre annuaire électronique central. En fournissant un large éventail de services s'appuyant sur une authentification centrale nous incitions les différentes composantes à injecter leurs usagers dans le SI de l'université. Le protocole Kerberos mis en œuvre dans plusieurs universités nous a beaucoup intéressés et répond à nos attentes. Il permet d'unifier l'authentification et de fournir un service compatible avec les différents systèmes d'exploitation. Fournir une authentification unique est une chose, faire en sorte qu'elle soit utilisée en est une autre. En déployant une solution de SSO² nous incitions l'ensemble des acteurs du SI à utiliser notre nouvelle authentification centrale.

Ainsi nous nous sommes appuyés sur l'annuaire OpenLDAP/Supann existant pour y adosser le nouveau service d'authentification Kerberos. Le principal phénomène que nous voulions endiguer est la multiplication des mots de passes (et parfois même des logins) de nos usagers. L'unification des authentifications nous permet d'avoir certains avantages, en plus du but initial :

- un seul référentiel pour les authentifications permet d'avoir un seul guichet d'accueil des utilisateurs pour l'ensemble de l'université ;
- les problèmes liés à l'authentification ne peuvent provenir que du système d'authentification unique. Les recherches des causes d'erreur sont restreintes à ce périmètre ;
- un seul référentiel d'authentification implique qu'il n'existe qu'un seul « compte utilisateur » pour chaque usager. Nous devons alors fournir un point d'accès unique aux utilisateurs leur permettant de modifier leur compte. Ce point d'accès unique peut alors faire l'objet d'une surveillance accrue ;

1. Centre de Ressources Informatiques Opérationnel en charge des salles informatiques d'enseignement.

2. SSO : Single Sign-On. Méthode d'authentification permettant à l'utilisateur de ne pas se ré-authentifier lors de l'ouverture d'une nouvelle application. L'authentification est faite une fois, on parle alors d'authentification unique.

- l'ensemble des applications web peuvent déléguer leur authentification à une source de confiance, permettant de ne pas redévelopper de nombreux (et peu mis à jour) modules d'authentification et de gestion des utilisateurs. Pour cette dernière fonctionnalité l'université utilise un serveur CAS³, nous souhaitons donc une technologie capable d'interagir avec un serveur CAS permettant une continuité du SSO.

Avec Kerberos la fonctionnalité de SSO système permet à l'utilisateur de pouvoir naviguer entre plusieurs machines sans se ré-authentifier. Intégré complètement au système Active Directory de Microsoft cette technologie permet également l'accès à des ressources informatiques (comme un répertoire partagé entre différents collaborateurs ou à des applications publiées par des serveurs TSE) sans qu'ils n'aient à ressaisir leur mot de passe. Cette technologie est compatible multi systèmes d'exploitation (elle est supportée par Windows, Linux et MacOS) ce qui permet d'intégrer l'ensemble des parcs informatiques de l'université.

Le protocole Kerberos lui-même permet de renforcer la sécurité autour des mots de passe. Comme le rapportait Nicolas Grenèche en 2011 [2], Le protocole Kerberos permet de limiter la circulation (en clair ou non) des mots de passe sur le réseau, tout en imposant un stockage fort du hash du mot de passe. L'article de Nicolas Grenèche nous éclaire également sur les différentes possibilités d'utilisation et d'intégration de ce protocole dans une université. Ce travail a été la base de toute réflexion pour nos travaux. Nous reviendrons sur l'architecture qu'il y propose et nous ajoutons un lien entre les différents mondes existants, d'un côté le monde Posix, de l'autre le monde Windows et les domaines Active Directory. Nous avons de plus travaillé sur les interactions entre le SSO Kerberos et le SSO CAS dans le domaine du web.

1.1 Kerberos en tant que SSO système

Dans [2] et [3] les auteurs décrivent comment installer et utiliser une authentification Kerberos pour différents systèmes. Nous laisserons certains détails techniques d'implémentation pour ne nous intéresser ici qu'aux fonctionnalités auxquelles nous pouvons arriver ainsi que leur aisance d'implémentation.

Les systèmes Unix utilisent les PAM et il existe un module PAM pour Kerberos. Dans sa configuration par défaut, ce module considère que si on arrive à obtenir un TGT, alors l'ouverture de session est autorisée. Il existe une autre possibilité, celle d'utiliser SSSD (voir [2] pour plus d'informations).

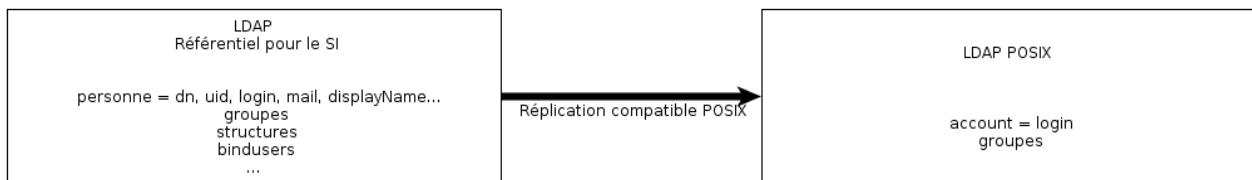


Figure 1 - Copie de certaines informations depuis l'annuaire central vers l'annuaire POSIX.

Les informations d'authentification sont contenues dans le serveur Kerberos, lequel s'appuie directement sur l'annuaire central. Un second annuaire, répliqua partiel de l'annuaire central, contenant les informations POSIX, comme les uid et les gid Unix, permet de servir une identité numérique minimale aux services les contactant. La réplique des informations est visible sur la figure 1.

L'authentification Windows est un peu plus complexe. En effet il est possible d'utiliser les « support tools »⁴ pour configurer directement l'interrogation du KDC, ou se relier à un domaine Active Directory. La première solution permet de rattacher un poste seul à notre solution d'authentification. La chaîne d'authentification est simple, l'utilisateur doit récupérer un ticket de service pour le poste sur lequel il souhaite ouvrir une session, s'il l'a il peut ouvrir sa session. La seconde méthode met en place une chaîne d'authentifications plus complexe mais permet de ne pas avoir à enrôler chaque nouvelle machine auprès du serveur Kerberos. On délègue ce travail au serveur Active Directory qui sait très bien le faire. Il faut utiliser des relations de confiance pour permettre l'authentification d'un utilisateur de notre royaume Kerberos sur notre Active Directory.

Nous avons considéré la question de la simplification de la gestion des parcs. Un parc est un ensemble de machines ayant un rôle similaire. Dans notre université nous dénombrons plusieurs parcs informatiques (pour les laboratoires de recherche,

3. CAS est un serveur d'authentification et de SSO pour les applications web. voir [4] pour plus d'informations.

4. voir http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/tools_overview.mspx?mfr=true

pour les services centraux, pour la présidence, pour les ressources humaines...). Chaque parc possède ses spécificités et ses gestionnaires. Nous souhaitons laisser une totale indépendance sur les machines pour les gestionnaires de parc, tout en conservant la totale maîtrise sur les identités numériques des usagers. Nous avons donc choisit la seconde solution.

Nous avons donc mis en place un domaine AD principal ayant pour vocation le relai des identités numériques et des authentications. Ce domaine est administré par la DSI et est prévu pour recevoir un ensemble de domaines enfants qui seront gérés par les gestionnaires de parc. Nous découplons ainsi la gestion dans un AD des utilisateurs, de la gestion des machines physiques. Nous assurons ici une continuité entre SSID Windows et identité numérique pour l'ensemble des parcs des domaines enfants. La gestion de l'identité numérique dans le monde windows est simplifiée. Grâce à des GPO positionnées sur le domaine parent ou sur les domaines enfants nous autorisons (ou non) les utilisateurs à se connecter aux postes. Ainsi, avec des domaines déployés dans l'ensemble de l'université, une seule identité numérique Windows est utilisée par un utilisateur, indépendamment de sa position géographique, pour ouvrir une session sur un poste de travail.

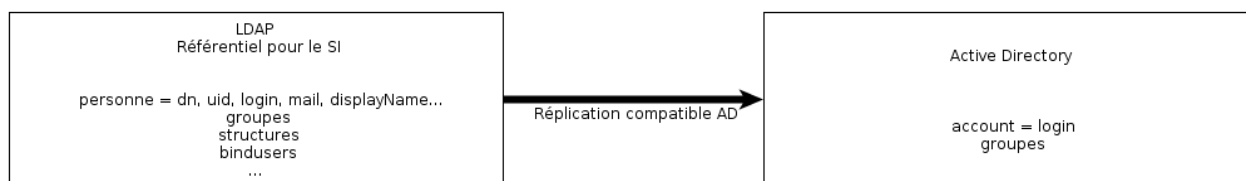


Figure 2 - Copie de certaines informations depuis l'annuaire central vers l'AD principal.

Les serveurs AD embarquent deux briques redondantes avec notre infrastructure principale : un annuaire LDAP et un serveur Kerberos. En positionnant correctement les méthodes de chiffrement entre notre serveur Kerberos et notre domaine AD nous arrivons à les faire communiquer, et à fournir des tickets pour nos utilisateurs Windows. Les identités numériques utilisées par Windows ne sont pas celles de notre annuaire principal mais sont une copie minimale des informations requises par l'AD comme l'on peut le voir sur la figure 2. Nous extrayons de l'annuaire central le nom du compte à créer, le principal associé ainsi que les groupes auxquels la personne appartient. Ces informations sont copiées dans l'AD et l'attribut `altSecurityIdentity` est positionné pour renvoyer le principal de l'utilisateur. Les postes joints aux domaines enfants sont alors configurés pour déléguer l'authentification au serveur Kerberos de l'université via GPO.

1.2 Intégration des services CAS et Kerberos

Le système de SSO Web CAS [4] permet l'authentification unique d'un utilisateur lors d'une session de navigation web. Lors de l'appel au CAS il est possible de paramétrer le client et le serveur pour qu'ils s'échangent des tickets Kerberos plutôt qu'un challenge et une réponse. La configuration côté client est relativement simple (hors configuration du poste pour qu'il puisse récupérer un ticket d'ouverture de session). Il s'agit de configurer le navigateur client pour qu'il négocie des tickets Kerberos avec le serveur CAS [3, 2].

Les trois navigateurs principaux sont aisément configurables. Firefox définit un paramètre contrôlant l'ensemble des sites web avec lesquels le navigateur peut négocier des tickets. De la même manière Chromium et Google-Chrome peuvent être lancés avec l'option permettant de définir le même ensemble de sites web. Enfin Internet Explorer, par défaut, autorise l'échange de tickets avec les zones qui lui sont déclarées de confiance (réglable par GPO).

Le serveur CAS peut lui être facilement configuré pour accepter les tickets Kerberos provenant d'un KDC renseigné. La configuration requise pour opérer cette communication est entièrement décrite sur le site web d'Esup [5]. Les configurations des différents navigateurs sont aisément trouvable sur l'Internet.

Nous avons rencontré un souci avec les dernières générations de navigateurs. Chromium et Internet Explorer, s'ils ne sont pas configurés pour négocier une authentification Kerberos, essaient absolument d'en obtenir une en demandant à l'utilisateur un login et un mot de passe, bloquant la navigation. Or, s'il est possible de maîtriser l'ensemble des navigateurs du parc interne, il est certainement impossible de maîtriser l'ensemble des navigateurs de la planète. Ce problème bloquant a été contourné en configurant plus finement notre CAS. Ce serveur ne tente une négociation Kerberos que si le navigateur en face est compatible. Les critères de compatibilité se basent sur le user-agent envoyé par le navigateur. Si le user-agent contient la chaîne Firefox ou Kerberos, alors on peut tenter une négociation. Les autres cas sont redirigés directement vers la bannière de login de l'utilisateur.

2 Mise en œuvre de l'infrastructure d'authentification

Dans cette partie nous allons décrire rapidement l'infrastructure que nous avons mise en place. Techniquement nous pouvons la découper en trois briques : une brique d'authentification (CAS, Kerberos, LDAP), une brique Active Directory, une brique de gestion des identités (Supann, module de gestion du compte).

2.1 La brique d'authentification

Le cœur du projet « Passeport Dauphine » est la brique d'authentification Kerberos. Kerberos permet l'utilisation du backend OpenLDAP, et comme nous souhaitons nous appuyer sur l'annuaire électronique central de l'université nous avons naturellement fait ce choix. L'installation doit être résiliente aux pannes ce qui nous a poussé à installer deux serveurs KDC, un maître et un esclave. Le KDC maître est séparé de son backend et inscrira ses informations dans l'annuaire électronique central. Le serveur KDC esclave est confondu avec son instance LDAP et sa réplication est assurée par des mécanismes LDAP.

Dans son article Nicolas Grenèche émet des objections à l'utilisation d'une telle configuration [2]. Nous utilisons cette configuration uniquement en interne. Nous nous protégeons grâce à d'autres serveurs esclaves, appauvris en informations, lorsque nous souhaitons les exposer à l'Internet.

De plus cette configuration possède un avantage certain, la résilience à la panne d'une machine. Si le serveur KDC maître tombe en panne, son backend reste disponible pour réplication, et si le backend tombe en panne, de toute façon il n'est plus possible d'utiliser le serveur maître. Le système de réplication prendra alors tout son sens, car les informations d'authentification auront effectivement été dupliquées. Les deux serveurs KDC surveillent donc de fait le serveur LDAP principal de l'université, avertissant les administrateurs de son indisponibilité. Si le serveur LDAP s'arrête, alors le KDC maître s'arrête, laissant l'ensemble des requêtes être satisfaites par le serveur esclave. Cette infrastructure est décrite par la figure 3.

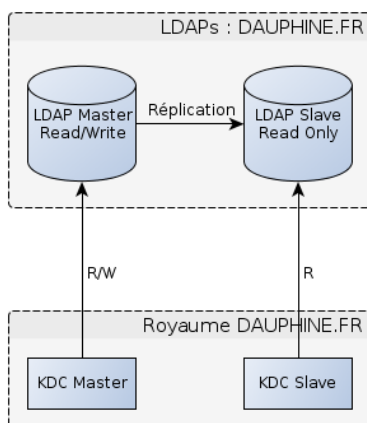


Figure 3 - Schéma de la brique Kerberos.

À cette brique Kerberos vient s'ajouter la brique d'authentification web CAS comme nous l'avons vu à la section 1.2

2.2 La brique de gestion des identités

Fournissant une infrastructure d'authentification unique et centrale, notre projet ne pouvait pas laisser de côté la problématique de la gestion du mot de passe par les utilisateurs. La mise en place d'une authentification centralisée a permis de repenser le module de modification des informations par les utilisateurs. Nous fournissons un point d'accès unique pour l'ensemble des utilisateurs leur permettant de réaliser les trois actions principales de gestion de leur mot de passe :

- activer son compte et choisir un mot de passe ;
- modifier son mot de passe ;
- réinitialiser son mot de passe en cas d'oubli.

La création d'un mot de passe (ou sa modification) n'est plus une opération bénigne. Le mot de passe de l'utilisateur est présent deux fois dans l'annuaire OpenLDAP : dans l'attribut traditionnel réservé au mot de passe LDAP des utilisateurs et dans l'attribut renseigné par le KDC lors de la création (ou la modification) du principal associé. La modification du mot de passe doit donc se faire de manière transactionnelle, de manière à assurer que l'annuaire est toujours dans un état cohérent. Cette opération transactionnelle est implémentée dans SupannLib [6, 7].

Nous pouvons gérer une autorisation particulière directement au niveau de l'authentification, il s'agit de l'autorisation d'authentification. Pour qu'il puisse se connecter un utilisateur doit disposer d'une fiche LDAP correctement remplie, de son login et de son mot de passe. Lors de l'authentification un challenge est envoyé au client qui fournira une réponse. La réponse attendue est calculée grâce à l'empreinte du mot de passe stockée en mémoire par l'annuaire. Si le service souhaitant une authentification ne peut accéder au hash du mot de passe, il est impossible de délivrer une authentification. À l'aide des ACLs LDAP nous implémentons le cycle de vie d'une fiche. Par exemple si un compte est marqué comme inactivé alors il sera impossible de s'authentifier avec.

La question de la confidentialité des données présentes dans notre annuaire LDAP se pose. La confidentialité des données au sein de notre annuaire principal est assuré par le mécanisme d'ACL de consultation. Nous avons profité de la refonte de l'annuaire (pour accepter le schéma Kerberos) pour revoir et renforcer l'intégrité des ACL sur l'annuaire.

Les attributs retournés par les serveurs CAS et Shibboleth sont maîtrisés par la DSI et réduits au strict besoin d'en connaître. La possibilité de moduler la configuration en fonction des serveurs appelants nous permet une certaine souplesse dans la gestion des autorisations tout en préservant les informations confidentielles. Nous n'exposons aucune donnée sensible sans que nous l'ayons choisi. Nous ne transmettons que le login des personnes, leur principal Kerberos et l'appartenance à des groupes aux annuaires répliqués. Nous ne transmettons jamais le mot de passe de l'utilisateur, nous déléguons toujours l'authentification à un partenaire de confiance.

L'infrastructure « Passeport Dauphine » n'a pas pour but la gestion des autorisations. Les autorisations sur les systèmes sont délégués aux gestionnaires de parcs et implémentées suivant les habitudes de chacun. L'infrastructure mise en place se limite à valider l'identité d'un utilisateur et à fournir l'ensemble des renseignements nécessaires pour la construction de l'autorisation au serveur appelant. L'autorisation d'accès à une partie d'un système de fichier pourra se baser sur l'appartenance à un groupe particulier.

2.3 Intégration de Kerberos et les briques POSIX et AD

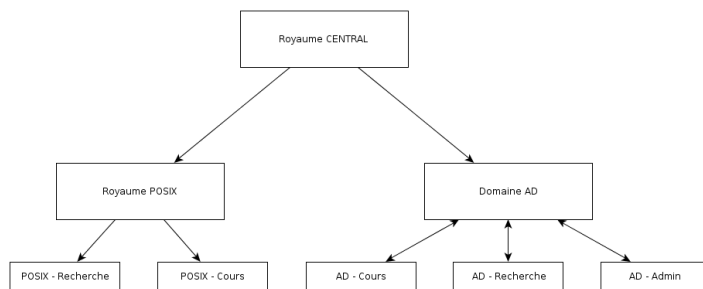


Figure 4 - Relations de confiance existantes entre les royaumes Kerberos et les domaines AD.

La figure 4 présente les différentes relations de confiance mises en place pour réaliser nos objectifs. Le royaume CENTRAL est servi par nos KDCs. Le domaine AD, qui comporte un royaume Kerberos, fait confiance au royaume CENTRAL, cette relation est nécessaire pour que les utilisateurs Windows puissent s'authentifier en tant qu'utilisateurs du royaume CENTRAL. Ces utilisateurs recevront un ticket CENTRAL qui sera accepté par le domaine AD. Chaque domaine enfant du domaine principal a une relation bilatérale de confiance, ceci permet aux utilisateurs du domaine parent de se connecter sur les machines du domaine enfant. Ainsi, les utilisateurs du royaume CENTRAL peuvent se connecter sur des machines des domaines enfants. Les mêmes mécanismes sont mis en jeu pour le royaume POSIX et d'éventuels autres royaumes placés en dessous. Les utilisateurs du royaume CENTRAL, se connectant sur une machine du royaume POSIX peuvent accéder aux services du domaine AD grâce à leur ticket d'authentification CENTRAL et les liens de confiance et réciproquement.

3 Déploiement – Accompagnement Utilisateurs

La principale difficulté est l'initialisation du principal Kerberos. Pour pouvoir utiliser l'infrastructure complète il faut que le compte de l'utilisateur soit enregistré dans le serveur de tickets Kerberos. L'enregistrement de l'utilisateur nécessite de transmettre le mot de passe de l'utilisateur au serveur Kerberos. Or il ne nous est pas possible de récupérer dans l'annuaire actuel l'ensemble des mots de passes des usagers pour les convertir directement. Nous devons donc demander aux usagers de changer leur mot de passe de manière à pouvoir utiliser les nouveaux services mis à disposition.

Pour rencontrer le plus grand succès possible nous avons mis en place un accompagnement des utilisateurs. Les utilisateurs doivent comprendre que l'intérêt du projet est de leur simplifier le quotidien. La plupart des utilisateurs de l'université n'arrive pas à faire la différence entre leur compte web, leur compte système, etc. Nous avons donc commencer par choisir un nouveau nom pour l'url du serveur CAS, de manière à renforcer l'idée qu'un changement était en cours. Le design de la mire d'authentification du CAS a été légèrement modifiée également pour refléter ce changement.

Dans un premier temps nous avons mis en production, au mois de juin, l'interface de gestion du compte sans communiquer autour. De cette manière nous avons capté l'intégralité des nouveaux arrivants à l'université. Nous avons pu valider que notre infrastructure était robuste et supportait la charge.

Nous avons alors communiqué à large échelle lors de la rentrée pour inciter les utilisateurs à migrer leur compte en « Passeport Dauphine » à l'aide de logos, d'affiches et de communications diverses. Nous avons mis en place des machines dédiées, en mode kiosque, permettant aux utilisateurs de changer leur mot de passe. Nous interceptons les tentatives de connexion au portail ENT de l'université. Si l'utilisateur n'a pas encore mis à jour son mot de passe nous le lui signifions et lui proposons de le faire maintenant. Enfin nous avons averti l'ensemble des utilisateurs du changement de la méthode d'authentification à l'université, en leur demandant de migrer leur compte en « Passeport Dauphine ». Il faut bien prendre garde à ne pas demander aux utilisateurs de changer leur mot de passe dans un mail. D'ailleurs certains utilisateurs ont signalé le message du service de la communication comme étant suspect et ont demandé conseil.

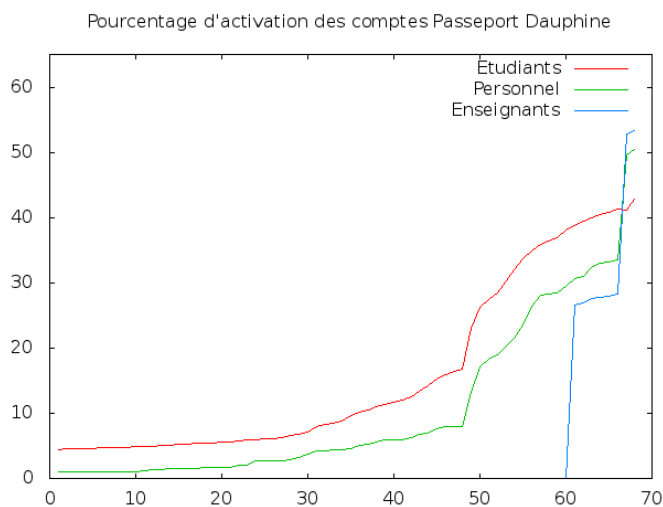


Figure 5 - Évolution du nombre de comptes « Passeport Dauphine ».

Suivant les populations le taux de changement de mot de passe varie. Sur la figure 5 nous présentons sur deux populations distinctes, les étudiants et les personnels de l'université, le nombre de « Passeport Dauphine » et le ratio à la population globale. Durant le mois d'août les seuls comptes « Passeport » sont ceux des étudiants nouvellement inscrits qui ont été activés directement comme « Passeport Dauphine ». Les personnels de l'université n'ont pas été sollicités pour migrer leur compte. La rentrée universitaire et la sollicitation des étudiants et des enseignants est visible sur le graphe. Le taux d'étudiant touché est cependant bien plus important que chez les personnels.

Globalement les personnels de l'université (enseignants, chercheurs et administratifs) sont les plus réticents à migrer leur compte vers un « Passeport Dauphine ». La raison principale est le changement de mot de passe.

Conclusion

Le projet n'est pas encore terminé, et il reste à cette heure de gros chantiers à mettre en route. L'ensemble des postes informatiques des administratifs doivent être migrés de notre domaine actuel vers les domaines nouvellement créés. Cette opération est prévue courant 2014. Ensuite il restera encore des évolutions possibles pour ce projet.

De par sa nature modulaire, nous envisageons d'étendre le concept à une fédération d'établissements d'enseignement, comme PSL. Le but sera qu'un étudiant d'un établissement de PSL puisse accéder aux ressources de Dauphine, permettant la libre circulation des étudiants dans la fédération. Cet état est possible en créant un nouveau royaume Kerberos et en accordant la confiance requise. La question de la cohabitation entre Kerberos et un système de mots de passes jetables (OTP) est aussi en cours de réflexion, menant à l'utilisation d'une authentification forte possible derrière un système de SSO. La création de différentes zones SSO de confiance plus ou moins élevées serait alors possible.

L'exemple le plus frappant de la réussite de ce projet est le cas des laboratoires de langues. Lors de la rénovation de ces salles nous avons mis à profit l'infrastructure d'authentification globale. Les systèmes authentifient l'utilisateur et offre l'accès à diverses ressources sans autre authentification : un espace réseau pour l'utilisateur, l'accès au logiciel utilisé pour les cours, l'accès à la plate-forme web de formation. Cette installation force les départements à enregistrer en temps et en heure les vacataires auprès des RH, ce qui nous permet de capter de nouvelles identités.

Ce projet a déjà porté des fruits intéressants. Il reste encore des services pouvant s'appuyer sur cette authentification unique à mettre en place. Le succès de ce projet tiendra dans l'offre de services qui l'accompagne.

Bibliographie

- [1] Laurent Mirtain. Ldap, 1999. <http://1999.jres.org/tutoriaux/ldap-cp.pdf>.
- [2] Nicolas Grenèche. (securely) kerberize my university. Dans *Actes de la conférence JRES2011*. https://2011.jres.org/archives/4/paper4_article.odt.
- [3] Guillaume Rousse. Kerberos, le sso universel. *GNU/Linux Magazine*, 143 :38–75, Novembre 2011.
- [4] Jasig cas. <http://www.jasig.org/cas>.
- [5] Pascal Aubry. Installation du serveur cas, 2010. <http://www.esup-portail.org/display/CASKERB/Installation+du+serveur+CAS>.
- [6] Lionel Lenoble Martial Lebec, Vincent Bruhier. Réalisation d'un webservice supann. Dans *Actes de la conférence JRES2011*, Toulouse, Décembre 2011. https://2011.jres.org/archives/178/paper178_article.pdf.
- [7] Supannlib : pour une gestion unifié des identités. Dans *Actes de la conférence JRES2013*, Montpellier, Décembre 2013.